UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
The person of Tracey D. Cox

Case No. 3:21MJ76

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE ATTACHMENT A

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252(a)(4)(B)	Possession of Child Pornography
18 U.S.C. § 2252A(a)(5)(B)	Possession of Child Pornography
18 U.S.C. § 2252(a)(2)	Receipt or Distribution of Child Pornography
18 U.S.C. § 2252A(a)(2)	Receipt or Distribution of Child Pornography

The application is based on these facts:

SEE ATTACHED AFFIDAVIT

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Kimberly.A.Wallace
Digitally signed by Kimberly.A.Wallace
Date: 2021.03.02 10:59:41 -05'00'

Applicant's signature

SA Kimberly Wallace, HSI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by FaceTime *(specify reliable electronic means).*

Date: 3/2/21

s signature

City and state: Dayton, Ohio

U.S. Magistrate Judge

ame and title

ATTACHMENT A

DESCRIPTION OF THE PERSON TO BE SEARCHED

The person of Tracey D. Cox, who is a black male, 48 years old, approximately 5'5" tall, last known weight of approximately 265 pounds, having black hair and brown eyes. The warrant includes authority to search Tracey D. Cox's person and any belongings carried by or in arms' reach of Tracey D. Cox, such as purses, wallets, bags, containers, and other items.

ATTACHMENT B

ITEMS TO BE SEARCHED AND SEIZED

Items evidencing violations of 18 U.S.C. §§ 2252(a)(2) and 2252A(a)(2) and (receipt and distribution of child pornography), and 18 U.S.C. §§ 2252(a)(4)(B) and 2252A(a)(5)(B) (possession of child pornography), including, but not limited to, the following:

Computers and Electronic Media

1. Any cellphones, computers, or computer hardware/media/software. The authorization includes the seizure and search of electronic data to include deleted data, remnant data and slack space. The seizure and search of cellphones, computers, and computer media will be conducted in accordance with the Affidavit submitted in support of this warrant.

2. Computer hardware, meaning any and all computer equipment, including any electronic devices that are capable of collecting, analyzing, creating, displaying, converting, storing, concealing, or transmitting electronic, magnetic, optical, or similar computer impulses or data. Included within the definition of computer hardware is any data processing hardware (such as central processing units and self-contained laptop or notebook computers); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical and compact disk storage devices, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); related communications devices (such as modems, cables and connections, recording equipment, RAM and ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone generating devices); any devices, mechanisms, or parts that can be used to restrict access to such hardware (such as physical keys and locks); cellular telephones and tablets; and digital cameras and recording devices.

3. Computer software, meaning any and all data, information, instructions, programs, or program codes, stored in the form of electronic, magnetic, optical, or other media, which is capable of being interpreted by a computer or its related components. Computer software may also include data, data fragments, or control characters integral to the operation of computer software, such as operating systems software, applications software, utility programs, compilers,

interpreters, communications software, and other programming used or intended to be used to communicate with computer components.

4. Computer-related documentation, meaning any written, recorded, printed, or electronically stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

5. Computer passwords and data security devices, meaning any devices, programs, or data -- whether themselves in the nature of hardware or software -- that can be used or are designed to be used to restrict access to, or to facilitate concealment of, any computer hardware, computer software, computer-related documentation, or electronic data records. Such items include, but are not limited to, data security hardware (such as encryption devices, chips, and circuit boards); passwords; data security software or information (such as test keys and encryption codes); and similar information that is required to access computer programs or data or to otherwise render programs or data into usable form.

6. Any computer or electronic records, documents, and materials referencing or relating to the above-described offenses. Such records, documents, or materials, as well as their drafts or modifications, may have been created or stored in various formats, including, but not limited to, any hand-made form (such as writing or marking with any implement on any surface, directly or indirectly); any photographic form (such as microfilm, microfiche, prints, slides, negative, video tapes, motion pictures, or photocopies); any mechanical form (such as photographic records, printing, or typing); any electrical, electronic, or magnetic form (such as tape recordings, cassettes, compact disks); or any information on any electronic or magnetic storage device (such as floppy diskettes, hard disks, CD-ROMs, optical disks, printer buffers, sort cards, memory calculators, electronic dialers, or electronic notebooks), as well as printouts or readouts from any magnetic storage device.

7. Any electronic information or data, stored in any form, which has been used or prepared for use either for periodic or random backup (whether deliberate, inadvertent, or automatically or manually initiated), of any computer or computer system. The form that such information might take includes, but is not limited to, floppy diskettes, fixed hard disks, removable hard disk cartridges, tapes, laser disks, CD-ROM disks, video cassettes, and other media capable of storing magnetic or optical coding.

8. Any electronic storage device capable of collecting, storing, maintaining, retrieving, concealing, transmitting, and using electronic data used to conduct computer or Internet-based communications, or which contains material or data obtained through computer or Internet-based communications, including data in the form of electronic records, documents, and materials, including those used to facilitate interstate communications, including but not limited to telephone (including mobile telephone) and Internet Service Providers. Included within this paragraph is any information stored in the form of electronic, magnetic, optical, or other coding on computer media or on media capable of being read by a computer or computer- related equipment, such as fixed disks, external hard disks, removable hard disk cartridges, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, laser disks, or other memory storage devices.

Computer and Internet Records and Physical Records

9. Any records related to the possession, receipt, and distribution of child pornography.

10. Any Internet or cellular telephone communications (including email, social media, online chat programs, etc.) with others in which child exploitation materials and offenses are discussed and/or traded.

11. Any Internet or cellular telephone communications (including email, social media, etc.) with minors.

12. Evidence of the utilization of peer-to-peer file sharing programs.

13. Evidence of utilization of email accounts, social media accounts, and online chat programs.

14. Evidence of the utilization of cloud or electronic storage.

15. Evidence of utilization of other usernames or aliases.

16. Records of personal and business activities relating to the operation and ownership of the computer systems, such as telephone records, notes (however and wherever written, stored, or maintained), books, diaries, and reference materials.

17. Any records or documents pertaining to accounts held with Internet Service Providers or of Internet use.

18. Records of address or identifying information for individuals using computers or devices seized from the person of Tracey D. Cox.

Materials Relating to Child Pornography, Child Erotica, and Depictions of Minors

19. Any child pornography.

20. Any and all visual depictions of minors.

21. Any and all address books, names, and lists of names and addresses of minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).

22. Any books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).

23. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).

24. Any and all child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids.

Other Records

25. Lists of computer and Internet accounts, including usernames and passwords.

26. Any information related to the use of aliases.

27. Documents and records regarding the ownership and/or possession of the items seized during the search of Tracey D. Cox.

28. Any records or documents pertaining to accounts held with Internet Service Providers or of Internet use.

Photographs of Search

29. During the course of the search, photographs of Tracey D. Cox may also be taken to record the condition and/or location of items seized from his person.

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF:	)	3:21MJ76
	)	**TO BE FILED UNDER SEAL**
THE PERSON OF TRACEY D. COX	)	

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Kimberly Wallace, Special Agent with Homeland Security Investigations, being duly sworn, depose and state as follows, to wit:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent ("SA") with the U.S. Department of Homeland Security, Homeland Security Investigations ("HSI"), and have been since 2010. As part of my daily duties as an HSI agent, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252(a) and 2252A. I have received training in the area of child pornography and child exploitation, and I have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. I have also participated in the execution of numerous search warrants involving child exploitation and/or child pornography offenses.

2. This Affidavit is made in support of an Application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the person of Tracey D. Cox, more fully described in Attachment A, for the things described in Attachment B.

3. The purpose of this Application is to seize evidence described in Attachment B of violations of Title 18 U.S.C. §§ 2252(a)(4)(B) and 2252A(a)(5)(B), which make it a crime to

possess child pornography and access child pornography with intent to view it, and violations of Title 18 U.S.C. §§ 2252(a)(2) and 2252A(a)(2), which make it a crime to receive and distribute child pornography.

4. As a federal agent, I am authorized to investigate violations of laws of the United States, and I am a law enforcement officer with the authority to execute warrants issued under the authority of the United States.

5. The statements in this Affidavit are based in part on information provided by other law enforcement officers and on my investigation of this matter. This Affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. Based on the facts in this Affidavit, I submit that there is probable cause to believe that contraband or evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252(a)(4)(B) and 2252A(a)(5)(B) (possession of or accessing with intent to view child pornography) and 18 U.S.C. §§ 2252(a)(2) and 2252A(a)(2) (receipt or distribution of child pornography) may be located on the person of Tracey D. Cox.

BACKGROUND ON COMPUTERS, E-MAIL, THE INTERNET AND ONLINE CHILD EXPLOITATION

6. Based upon my knowledge, training and experience in online child exploitation and child pornography investigations, as well as the experience and training of other law enforcement officers with whom I have had discussions, I have learned the following:

a. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, stored, and communicated as a commodity and a further tool of online child exploitation. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Individuals can transfer photographs from a camera onto a computer-readable format with a variety of devices, including scanners, memory card readers, or directly from digital cameras. When a digital photo is taken, it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera or smartphone to the computer. In the last ten years, the resolution of pictures taken by digital cameras and smartphones has increased dramatically, meaning that such pictures have become sharper and crisper. Photos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards often store up to 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.

c. Modems allow computers to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTPs) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., “instant messaging”), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

d. The capability of a computer to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on the computer. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. CDs and DVDs are unique in that special software must be used to save or "burn" files onto them. Media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet, the World Wide Web, and other Internet components afford individuals many different and relatively secure and anonymous venues for obtaining, viewing and trading child pornography or for communicating with others to do so or to entice children.

f. Individuals can use online resources to retrieve, store, and share child pornography, including services offered by Internet Portals such as Google, America Online ("AOL"), Yahoo! and Hotmail, among others. Online services allow a user to set up an account providing e-mail and instant messaging services, as well as electronic

storage of computer files in any variety of formats. A user can set up an online storage account from a computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. And even in cases where online storage is used, evidence of child pornography can be found on the user's computer in many cases.

g. As is the case with most digital technology, computer communications can be saved or stored on hardware and computer storage media used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. However, digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained for very long periods of time until overwritten by other data.

i. The interaction between software applications and the computer operating systems often results in material obtained from the Internet being stored multiple times, and even in different locations, on a computer hard drive without the user's knowledge. Even if the computer user is sophisticated and understands this automatic storage of information on his/her computer's hard drive, attempts at deleting the material often fail because the material may be automatically stored multiple times and in multiple locations within the computer media. As a result, digital data that may have evidentiary value to this investigation could exist in the user's computer media despite, and long

after, attempts at deleting it. A thorough search of this media could uncover evidence of receipt, distribution and possession of child pornography. Data that exists on a computer is particularly resilient to deletion.

BACKGROUND ON CELLULAR PHONES AND ONLINE CHILD EXPLOITATION

7. Based upon my knowledge, training and experience in online child exploitation and child pornography investigations, as well as the experience and training of other law enforcement officers with whom I have had discussions, I have learned the following:

a. Cellular telephones have revolutionized the way in which child pornography is produced, distributed, stored, and communicated as a commodity and a further tool of online child exploitation.

b. Generally speaking, a cellular telephone is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A cellular telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, cellular telephones offer a broad range of capabilities, including certain capabilities traditionally associated with desktop and laptop computers. These capabilities include: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information

from the Internet. Cellular telephones may also include global positioning system ("GPS") technology for determining the location of the device.

c. The capability of a cellular telephone to store and transfer images in digital form makes the cellular telephone itself an ideal repository for child pornography. As explained further below, the storage capacity of electronic media used in home cellular telephones has increased tremendously within the last several years. These drives can store extreme amounts of visual images at very high resolution.

d. The Internet, the World Wide Web, and other Internet components afford individuals many different and relatively secure and anonymous venues for obtaining, viewing and trading child pornography or for communicating with others to do so or to entice children.

e. Individuals can use online resources to retrieve, store and share child pornography, including services offered by Internet Portals such as Google, America Online (AOL), Yahoo! and Hotmail, among others. Online services allow a user to set up an account providing e-mail and instant messaging services, as well as electronic storage of cellular telephone files in any variety of formats. A user can set up an online storage account from any cellular telephone with access to the Internet. Evidence of such online storage of child pornography is often found on the user's cellular telephone. And even in cases where online storage is used, evidence of child pornography can be found on the user's cellular telephone in most cases.

f. The interaction between software applications and the cellular telephone operating systems often results in material obtained from the Internet being stored multiple times, and even in different locations, on a cellular telephone hard drive without the user's

knowledge. Even if the cellular telephone user is sophisticated and understands this automatic storage of information on his/her cellular telephone's storage, attempts at deleting the material often fail because the material may be automatically stored multiple times and in multiple locations within the cellular telephone media. As a result, digital data that may have evidentiary value to this investigation could exist in the user's cellular telephone media despite, and long after, attempts at deleting it. A thorough search of this media could uncover evidence of receipt, distribution, and possession of child pornography.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO PRODUCE, DISTRIBUTE, POSSESS, AND/OR RECEIVE CHILD PORNOGRAPHY

8. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who produce, distribute, possess, and/or receive child pornography.

a. These individuals may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. These individuals may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Such individuals oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. To the extent that these individuals possess and maintain "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., they often maintain those hard copies in the privacy and security of their home or some other secure location. These individuals typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, these individuals often maintain their collections that are in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area, or in a cellular telephone. These collections are often maintained for several years and are kept close by, usually at the individual's residence, to enable the collector to view the collection, which is valued highly. With the growth of the Internet, a large percentage of most collections today are in digital format. Increasingly, individuals are utilizing laptop computers and other smaller devices, such as cellular telephones, iPads, and tablets, to do their computing. It is not uncommon for individuals involved in child pornography offenses to use multiple devices to obtain, store, or share their collections.

e. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis; however, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools.

f. These individuals may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

g. These individuals refer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

BACKGROUND ON NCMEC

9. The National Center for Missing and Exploited Children (NCMEC), among other things, tracks missing and exploited children, and serves as a repository for information about child pornography. Companies that suspect that child pornography has been stored or transmitted on their systems can report that information to NCMEC in a cybertip. To make such a report, a company providing services on the internet, electronic service providers ("ESPs") and internet service providers ("ISPs"), can go to an online portal that NCMEC has set up for the submission of these tips. The ISP or ESP then can provide to NCMEC information concerning the child exploitation activity it believes to have occurred, including the incident type, the incident time, any screen or user names associated with the activity, any IP address or port numbers it captured, as well as other information it may have collected in connection with the suspected criminal activity. The ISP or ESP may also upload to NCMEC any files it collected in connection with the activity. Using publicly available search tools, NCMEC then attempts to locate where the activity occurred based on the information the ISP or ESP provides, such as IP addresses. NCMEC then

packages the information from the ISP and ESP along with any additional information it has, such as previous related cybertips, and sends it to law enforcement in the jurisdiction where the activity is thought to have occurred.

BACKGROUND ON KIK

10. Kik is a mobile application designed for chatting or messaging. To use this application, a user downloads the application to a mobile phone or other mobile device via a service such as Google Play Store, Apple iTunes, or another similar provider. Once downloaded and installed, the user is prompted to create an account and username. The user also has a display name, which is what other users see when transmitting messages back and forth. Once the user has created an account, the user is able to locate other users via a search feature, and the two parties can then send each other messages, images, and videos.

11. Kik users are also able to create chat groups with a limited number of individuals to communicate in a group setting and exchange images and videos. These groups are administered by the group creator who has the authority to remove and ban other users from the created group. Once the group is created, Kik users have the option of sharing a link to the group that includes all of their contacts or any other user. These groups are frequently created with a "hashtag" that is easily identifiable or searchable by keyword in Kik.

DROPBOX BACKGROUND

12. Dropbox is a service that allows its users to store files on Dropbox's servers. As reflected in the Dropbox Privacy Policy[1] posted on December 17, 2019 and effective on January 1, 2020:

[1] The Dropbox Privacy Policy is available at https://www.dropbox.com/privacy.

a. Dropbox's services "are designed as a simple and personalized way for you to store your files, documents, photos, comments, messages, and so on ('Your Stuff'), collaborate with others, and work across multiple devices and services."

b. Dropbox stores, processes, and transmits "Your Stuff as well as information related to it. This related information includes your profile information that makes it easier to collaborate and share Your Stuff with others, as well as things like the size of the file, the time it was uploaded, collaborators, and usage activity."

c. Dropbox also collects "information related to how you use the Services, including actions you take in your account (like sharing, editing, viewing, creating and moving files or folders)."

d. In addition, Dropbox collects "information from and about the devices you use to access the Services. This includes things like IP addresses, the type of browser and device you use, the web page you visited before coming to our sites, and identifiers associated with your devices."

e. Dropbox also collects "the information you provide to us when you do things such as sign up for your account, upgrade to a paid plan, and set up two-factor authentication (like your name, email address, phone number, payment info, and physical address)."

PROBABLE CAUSE

13. In approximately June of 2018, HSI D.C., acting in an undercover capacity on Kik, began monitoring certain chat activity. During the monitoring timeframe, a Kik user with the username "Blkfatswag" posted child exploitation material on the following approximate dates and times:

a. On or about July 8, 2018 at 16:53 UTC, an image which depicts two Asian females who are performing oral sex on a male. One of the females is wearing a light blue hair

clip in her hair, and she appears to be a minor and has her mouth on the base of the male's penis.

b. On or about September 22, 2018 at 14:36 UTC, an image which depicts a minor female with her tongue out as an adult male ejaculated on her face.

c. On or about October 2, 2018 at 14:24 UTC, a video which depicts a black minor female performing oral sex on a white male.

d. On or about October 8, 2018 at 11:23 UTC, an image which depicts a minor female performing oral sex on two adult males. One male is sitting on a bed and the other male is lying on his back with his legs near the sitting male.

14. On or about August 17, 2018, September 28, 2018, and May 29, 2019, Kik was served with an administrative subpoena/summons for subscriber information related to username "Blkfatswag." A review of the results obtained revealed a name of "John Conners" and a confirmed email address of johnislit03@gmail.com.[2] The account registered a device on approximately May 1, 2018 which was an Android model SM-J327P. Another device registered on the account on approximately March 28, 2019 was an Android model SM-G960U.

15. On or about October 10, 2018, Google was served with an administrative subpoena/summons for subscriber information related to account johnislit03@gmail.com. A review of the results from Google revealed a name of "John Conners" with an account creation date of February 24, 2018. Account services listed for johnislit03@gmail.com included Android, Gmail, Google Calendar, Location History, Minutemaid, and Web & App Activity.

[2] Several IP addresses were included in subscriber information for the results obtained for the 2018 subpoena/summons returns for "Blkfatswag". Subpoena/summons were sent to the provider for the IP addresses included for "Blkfatswag" and the returns stated that no subscriber information was available.

16. IP addresses for logins were also provided by Google for johnislit03@gmail.com. A subpoena/summons was sent to the provider for the IP addresses included for johnislit03@gmail.com and the return stated that no subscriber information was available.

17. In March 2019, an open internet query was conducted for the username "Blkfatswag," which resulted in an associated Tumblr account for "bigblk77." Posts on this Tumblr account, "bigblk77", self-identified as Kik username "Blkfatswag."

18. On or about April 5, 2019, Tumblr was served with a subpoena/summons for subscriber information for account "bigblk77." Tumblr responded with account information for "bigblk77," which included an email address of traceyc375@gmail.com.

19. On or about May 21, 2019, Google was served with a subpoena/summons for subscriber information for account traceyc375@gmail.com. Google responded with account information for traceyc375@gmail.com, which included a name of Tracey Cox, a number of 937-732-1190, a recovery email address of trae237@yahoo.com, and several IP addresses. Account services listed for traceyc375@gmail.com included Android, Android Device Console, Device Centric Auth, Gmail, Google Calendar, Google Chrome Sync, Google Docs, Google Hangouts, Google Keep, Google My Maps, Google Payments, Google Photos, Location History, Web & App Activity, YouTube. In addition, the information provided by Google indicated included a login IP address of 2600:1:91cb:f648:b1f7:933d:d919:ab6b for May 17, 2019.

20. On or about June 27, 2019, Sprint was served with a subpoena/summons for subscriber information for telephone number 937-732-1190. Sprint responded with subscriber information of Tracey Cox at 23 S Findlay St, Dayton, OH 45403.

21. On or about June 27, 2019, Sprint was served with a subpoena/summons for subscriber information for IP address 2600:1:91cb:f648:b1f7:933d:d919:ab6b for May 17, 2019 which was

utilized to login to traceyc375@gmail.com. Sprint responded with subscriber information of Tracey Cox at 23 S Findlay St, Dayton, OH 45403.

22. On or about August 16, 2019, a query in a law enforcement database for Tracey Cox in Montgomery County, Ohio revealed a driver's license for Tracey Cox, with a residence address of 23 S Findlay St, Dayton, OH 45403. The query revealed that a member of the Ohio Internet Crimes Against Children ("ICAC") had also queried the driver's license for Cox in August of 2019.

23. I contacted Ohio's ICAC to deconflict HSI's investigation regarding Cox. Ohio's ICAC provided me with a CyberTipline Report (51818877) from NCMEC.

a. On or about July 5, 2019, Google, an ESP, submitted information to NCMEC. Google classified the incident type as child pornography. The CyberTipline Report included basic subscriber information, which included a name of Tracey Cox, an email address of traceyc375@gmail.com, and a telephone number of 937-732-1190. The CyberTipline Report included three (3) uploaded files for the reported account, traceyc375@gmail.com. The file bearing file name c63a26c5-ba90-483c-bcda-f78c2b70c888.jpg was viewed by the ESP.

b. I viewed c63a26c5-ba90-483c-bcda-f78c2b70c888.jpg, and it is an image depicting a black female, who appears to be a minor based on a lack of physical development, facing the camera and wearing only socks while squatting on the floor with her hands on her hips and her legs spread to reveal her genitals.

24. On or about November 27, 2019, I applied for and was granted a search warrant, issued in the Southern District of Ohio, for certain information stored at premises owned, maintained, controlled, or operated by Google associated with accounts traceyc375@gmail.com and johnislit03@gmail.com.

25. On or about December 16, 2019, Google responded to the above-referenced search warrant. My review of information provided by Google in response to the search warrant is summarized, in substance and in part, as follows:

a. Subscriber information for account traceyc375@gmail.com included, among other things, a name of Tracey Cox, a status of disabled, and an end of service date of July 5, 2019. The recovery email was listed as trae237@yahoo.com.

b. IP logs indicated that IP address 2600:1:91aa:f266:e44b:dff1:991c:3e7 was used to login to account traceyc375@gmail.com on February 3, 2019 at 22:22:45 UTC and account johnislit03@gmail.com on February 3, 2019 at 22:22:46 UTC.

c. Pertinent information located in email correspondence for account johnislit03@gmail.com included one email from Kik received on February 24, 2018 which stated in part, "Your username is: Blkfatswag".

d. Pertinent information located in email correspondence for account traceyc375@gmail.com included:

i. An email from Tumblr on or about January 12, 2018 addressed to "bigblk77".

ii. At least two emails in account traceyc375@gmail.com identified Tracey Cox as the account holder.

1. On or about July 24, 2017, traceyc375@gmail.com sent an email signed "Tracey D. Cox" with the subject "New hire paperwork." Attached to the email was paperwork that included, among other things, a name of Tracey Darnell Cox, a phone number of 937-732-1190, and an address of 23 S. Findlay St., Dayton, OH 45403.

2. On or about May 14, 2018, traceyc375@gmail.com was copied on an email attaching a resume for Tracey Cox that included a phone number of 937-732-1190, an email address of trae237@yahoo.com, and an address of 23 S. Findlay Street, Dayton, Ohio 45403.

iii. An email from Google on or about March 30, 2019, which stated in part, "Google received a request to use this email address to help recover Google Account johnislit03@gmail.com."

e. Traceyc375@gmail.com sent multiple messages to different accounts ending in "@profiles.google.com". For example, in one message from on or about May 16, 2019, traceyc375@gmail.com provided a full name of "Tracey Darnell Cox". In other messages from on or about June 13, 2019, traceyc375@gmail.com stated, "I just bought this phone back in April," and identified the phone as a "Galaxy S-9".

f. A Google Photos folder for account traceyc375@gmail.com contained multiple subfolders which appeared to be titled with dates. For instance:

i. A folder labeled "2015-11-04" contained a video bearing file name 4_226812884984791153.mp4 that depicted an adult male's penis anally penetrating a prepubescent female.

ii. A folder labeled "2019-05-18" contained at least two (2) different selfie images of Tracey Cox titled "image-20190518_121325.jpg" and "image-20190518_140549.jpg" (this was determined because the selfie images appeared to be the same person depicted in the Ohio driver's license photograph for Cox). Also located in the folder were excel spreadsheets titled "image-20190518_121325.jpg.csv" and "image-20190518_140549.jpg.csv". The

spreadsheets contained multiple columns of information which appeared to be file data related to the selfie images with corresponding titles. The column labeled "EXIF - Camera Model" for both spreadsheets contained "SM-G960U".

iii. A folder labeled "2019-07-03" contained several videos that depicted child pornography.

1. One file was a video bearing file name f07fe417-0970-46f7-a1ca-5430f263877b.mp4 that depicted a prepubescent female straddling an adult male, with her lower bathing suit pulled to the side, being vaginally penetrated by the adult male.

26. On or about May 12, 2020, I contacted NCMEC to deconflict HSI's investigation regarding Cox. Approximately a day later, NCMEC responded and referenced a CyberTipline Report (71128369) related to traceyc375@gmail.com. I obtained the report, which is further detailed below.

a. On or about April 27, 2020, Dropbox, Inc., an ESP, submitted information to NCMEC. Dropbox classified the incident type as child pornography. The CyberTipline Report included basic subscriber information, which included an email address of traceyc375@gmail.com, a screen/user name of Tracey Cox, and an ESP user ID of 2067085136. The CyberTipline Report included four (4) uploaded files. All of the files were viewed by the ESP, including a file bearing file name 5E868A35-DA29-4492-8189-B489FDD493CB.MOV.

b. I viewed 5E868A35-DA29-4492-8189-B489FDD493CB.MOV, and it is a video containing multiple clips of different people. Several excerpts from the video include the following:

i. An individual digitally penetrating a prepubescent female's vagina.

ii. An individual performing fellatio on a prepubescent male.

iii. A prepubescent male and prepubescent female having intercourse.

27. On or about July 27, 2020, I was contacted by NCMEC regarding a CyberTipline Report (74802408) possibly related to the instant investigation related to Tracey Cox. I obtained the report, which is further detailed below.

a. On or about July 15, 2020, Dropbox, Inc., an ESP, submitted information to NCMEC. Dropbox classified the incident type as child pornography. The CyberTipline Report included basic subscriber information, which included an email address of trae237@yahoo.com, a screen/user name of Tracey Cox, and an ESP user ID of 455190637. The CyberTipline Report included a login IP address of 2600:1:9122:7d44:95a:68b7:736e:3c50 for May 14, 2020. The CyberTipline Report listed 43 uploaded files.[3] All of the files were viewed by the ESP, including a file named 3e428f6b-fd61-4446-b99b-9c9bb5c7013a_ogfyeopntmmetge3_glgla.mp4.

b. I viewed 3e428f6b-fd61-4446-b99b-9c9bb5c7013a_ogfyeopntmmetge3_glgla.mp4, and it is a video depicting a naked female toddler performing fellatio on an adult male and an adult male using his hand and penis to rub the female toddler's vagina and anally penetrating the female toddler with his penis.

28. On or about July 28, 2020, Sprint was served with a subpoena/summons for IP address 2600:1:9122:7d44:95a:68b7:736e:3c50 for May 14, 2020. Sprint responded with subscriber information of Tracey Cox at 23 S Findlay St, Dayton, OH 45403.

[3] One video file appeared to be a duplicate entry in the CyberTipline Report since one file name was listed twice and only 42 files were actually attached to the Report.

29. On or about August 28, 2020, I applied for and was granted a search warrant, issued in the Southern District of Ohio, to Dropbox for information associated with accounts associated with (1) User ID 2067085136 and email address traceyc375@gmail.com and (2) User ID 455190637 and email address trae237@yahoo.com.

30. On or about September 1, 2020, Dropbox responded to the above-referenced search warrant. My review of information provided by Dropbox in response to the search warrant is summarized, in substance and in part, as follows:

a. Mobile information was included in subscriber information for both accounts. A review of the mobile information included a device model of SM-G960U for Dropbox account traceyc375@gmail.com (User ID 2067085136) on April 23, 2020 and for Dropbox account trae237@yahoo.com (User ID 455190637) on July 1, 2020. Dropbox account trae237@yahoo.com (User ID 455190637) also included a device model of SM-J327P registered on August 23, 2018 and January 26, 2019.

b. Dropbox account content associated with traceyc375@gmail.com included multiple files depicting child pornography. Description of one (1) file is as follows:

    i. A video (file name VID-20180424-WA0088.mp4) depicted an individual performing fellatio on a prepubescent male's penis.

c. Dropbox account content associated with trae237@yahoo.com included:

    i. A folder titled "Camera Uploads". The folder contained multiple files, including six (6) files that appeared to be selfie images of Tracey Cox (this was determined because the selfie images appeared to be the same person depicted in the Ohio driver's license photograph for Cox); and

ii. A folder titled "New folder" that contained multiple files depicting child pornography. Description of one (1) file is as follows:

1. A video (file name 5eba6ccc-12d5-4590-9601-3cdc0548fc7b.mp4) depicted two prepubescent females, with their dresses pulled up revealing their genitals, fondling each other.

31. On or about October 1, 2020, Dayton Power and Light (DPL) was served with a subpoena/summons for account/customer information for address 23 S. Findlay St, Dayton, OH 45403. DPL responded with a name (hereinafter referred to as "Individual 1"), personal identifying information ("PII"), and a telephone number for the customer. A driver's license query for Individual 1 (which matched the same PII as listed in the DPL return) listed a different residential address for Individual 1.

32. On or about January 13, 2021, another HSI SA and I traveled to 23 S. Findlay St, Dayton, OH. Two occupants at the residence stated that Tracey Cox no longer lived at the residence. The other HSI SA and I then traveled to the address listed on Individual 1's driver's license. No one responded to repeated knocks on the door, I left a business card which contained various contact methods. Later that day, I received a telephone call from a male who claimed to be Individual 1. The telephone number that Individual 1 called from was the same telephone number listed in customer information received in the return from DPL. Individual 1 stated, in substance and in part, that Individual 1 owned 23 S. Findlay Street and that Cox recently moved out of the house. Individual 1 provided me with a current address of 1429 Wilmington Ave, Apt 108 for Cox.

33. On or about January 13, 2021, the other HSI SA and I traveled to 1429 Wilmington Ave, Apt 108, Dayton, Ohio 45420. Tracey Cox answered the door to apartment 108. The other HSI SA and I identified ourselves and presented law enforcement credentials. We spoke to Cox from

the hallway outside the apartment while Cox remained inside the apartment. During the course of the conversation, Cox stated, in substance and in part, the following:

a. Cox currently utilized a Galaxy mobile phone that he purchased in approximately March 2018.

b. Cox accessed the internet via his mobile phone service.

c. No one other than Cox had utilized his mobile phone.

d. Cox's mobile phone number was 937-732-1190.

34. On or about March 1, 2021, Colonial Court was served with a subpoena/summons for the current occupant(s) of 1429 Wilmington Ave, Apt 108, Dayton, Ohio 45420. The office manager stated that Tracey Cox is the current occupant and provided the lease application. The application stated, in substance and in part, that the assigned address was "1429-108" for a term of one year starting on December 1, 2020. Contact information for Cox listed a telephone number of 937-732-1190.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

35. This Application seeks permission to search for certain records that might be found on the person of Tracey D. Cox, in whatever form they are found. One form in which the records are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of computers and electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

36. Given the information set forth above, I submit that if a computer or electronic storage medium is found on Tracey D. Cox, there is probable cause to believe those records referenced above may still be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

37. As further described in Attachment B, this Application seeks permission to locate not only computer files and electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on any computer or electronic storage medium on the person of Tracey D. Cox because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online usernames, nicknames, and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of

session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the

offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an

instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

38. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of a person it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process that requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage

devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it may be impractical to search for data during the execution of the physical search of the person; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

39. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying computers and electronic storage media

that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

SEARCH METHODOLOGY TO BE EMPLOYED

40. All computers, other computer hardware, computer software, and any form of electronic storage media that could contain evidence described in this warrant may be seized for an off-site search for evidence that is described in the attachments of this warrant. It is anticipated that mirror copies or images of such evidence will be made if the failure to do so could otherwise potentially alter the original evidence.

41. The search procedure of electronic data contained in computers, other computer hardware, computer software, and/or electronic storage media may include the following techniques (the following is a non-exhaustive list, as other search procedures may be used):

a. On-site triage of computer systems to determine what, if any, peripheral devices or digital storage units have been connected to such computer systems, a preliminary scan of image files contained on such systems and digital storage devices to help identify any other relevant evidence or potential victims, and a scan for encryption software;

b. On-site forensic imaging of any computers that may be partially or fully encrypted, in order to preserve unencrypted electronic data that may, if not immediately imaged on-scene, become encrypted and accordingly unavailable for examination; such imaging may require several hours to complete and require law enforcement agents to secure the search scene until that imaging can be completed;

c. Examination of all of the data contained in such computers, other computer hardware, computer software, or electronic storage media to view the data and determine whether that data falls within the items to be seized as set forth herein;

d. Searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

e. Surveying various file directories and the individual files they contain;

f. Opening files in order to determine their contents;

g. Scanning storage areas;

h. Performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and

i. Performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

42. Contextual information necessary to understand the evidence, to identify the user/possessor of the child pornography, and to establish admissibility of the evidence in subsequent legal proceedings will also be sought by investigative agents.

43. Because it is expected that the computers, other computer hardware, computer software, and any form of electronic storage media may constitute (1) instrumentalities of the offense, (2) fruit of criminal activity, (3) contraband, or (4) evidence otherwise unlawfully possessed, it is

anticipated that such evidence will not be returned to the owner and that it will be either forfeited or ultimately destroyed in accordance with the law at the conclusion of the case.

a. Because of the large storage capacity as well as the possibility of hidden data within the computers, other computer hardware, and any form of electronic storage media, it is anticipated that there will be no way to ensure that contraband-free evidence could be returned to the user/possessor of the computer, other computer hardware, or any form of electronic storage media, without first wiping such evidence clean. Wiping the original evidence clean would mean that the original evidence would be destroyed and thus, would be detrimental to the investigation and prosecution of this case.

b. Further, because investigators cannot anticipate all potential defenses to the offenses in this Affidavit, and as such, cannot anticipate the significance of the evidence that has been lawfully seized pursuant to this warrant, it is requested that all seized evidence be retained by law enforcement until the conclusion of legal proceedings or until other order of the court.

44. If after careful inspection investigators determine that such computers, other computer hardware, computer software, and electronic storage media do not contain or constitute (1) instrumentalities of the offense, (2) fruit of criminal activity, (3) contraband, (4) evidence otherwise unlawfully possessed, or (5) evidence of the person who committed the offense and under what circumstances the offense was committed, then such items seized will be returned.

CONCLUSION

45. Based on the above information, there is probable cause to believe that 18 U.S.C. §§ 2252(a)(2) and 2252A(a)(2) (distribution and receipt of child pornography) and 18 U.S.C. §§ 2252(a)(4)(B) and 2252A(a)(5)(B) (possession of child pornography) have been violated, and that the

property, evidence, fruits, and/or instrumentalities of these offenses listed in Attachment B, which is incorporated herein by reference, may be located on the person of Tracey D. Cox.

46. Based upon the foregoing, I respectfully request that this Court issue a search warrant for the person of Tracey D. Cox, more particularly described in Attachment A, authorizing the seizure of the items described in Attachment B.

Respectfully submitted,

Kimberly.A.Wallac Digitally signed by Kimberly.A.Wallace Date: 2021.03.02 11:00:23 -05'(

Kimberly Wallace
Special Agent
Homeland Security Investigations

Subscribed and sworn before me this 2nd day of March 2021.

Sharon L. Ovington
United States Magistrate Judge